

REMARKS

Applicants appreciate the thorough examination of the present application as evidenced by the Office Action. Applicants submit the present application is in form for allowance for at least the reasons discussed below.

The Claim Objections:

Claims 1-25 are objected to because of various alleged informalities in Claims 1, 3, 7, 9, 12, 13, 19 and 25. Office Action, pp. 2-3. To expedite prosecution of this application, the amendments suggested by the Examiner have been included in the amended claims. Accordingly, Applicants request withdrawal of the objection as obviated.

The Prior Art Rejections:

Claims 1-8, 12-20 and 25 stand rejected as anticipated under 35 U.S.C. § 102(e) over United States Patent Application Publication No. 2003/01201593 to Bansal *et al.* ("Bansal"). Office Action, p. 3. Claims 9-10 and 21-23 stand rejected as obvious under 35 U.S.C. § 103 over Bansal in light of United States Patent No. 5,991,882 to O'Connell ("O'Connell"). Office Action, p. 11.

Independent Claims 1, 13 and 25 Are Patentable:

In rejecting independent Claim 1, among other things, the Office Action asserts that Bansal at paragraph 423 discloses account privileges management as a "user can subscribe to content" and that paragraph 424 discloses a confirmation request that can be "seen as a challenge question since the user is required to act upon the request to confirm the user's identity." Office Action, pp. 4-5. Applicants disagree.

As an initial matter, paragraph 423 of Bansal relates to a user registering for a "subscription management service" that sends "categorized e-mail to a managed distribution list." In other words, a user acts to add him or her self to a listserv so that they will be included on the distribution list and receive associated notifications and the like sent to subscribers to the list. Bansal, Paragraphs 419-423. As further described at paragraph 424, a

In re: Lineman
Serial No.: 01/696,098
Filed: October 29, 2003
Page 9

confirmation may be required to help "prevent anonymous or unauthorized subscriptions." In other words, this section would appear to indicate the system, after receiving a request, may send an email to a known email associated with the request and await a reply to confirm it was actually that user that submitted the request.

In contrast, Claim 1 recites a receiving a request associated with "password and/or account privileges management." As is clear from the definitions for "privileges (referring to access privileges)" in the Microsoft Computer Dictionary (copy of excerpts attached) and the use of this term, for example, in the publication, DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria" (printout of excerpts of this and other webpages using the term attached), "privileges" refer to security related features of what a user account may access, not to what they choose to access using those privileges. In contrast, as discussed above, paragraph 423 of Bansel merely relates to registration for a listserv that the user presumably already had privileges to use. Thus, subscribing for a list, contrary to the assertion in the Office Action, cannot be reasonably interpreted as "account privileges management." Final Action, p. 4. Accordingly, the rejection of independent Claim 1 and the claims depending therefrom should be withdrawn for at least these reasons.

Furthermore, Claim 1 also recites a responsive query including a "challenge question to validate" a user request to a network password and/or account privileges management self-service application. In other words, the validation is used responsive to a user attempting to access the self-service application. As further recited in Claims 9 and 10, the response to the challenge then controls access to services of the application. In contrast, the cited sections of Bonsel are addressed to confirming that a request to be added to a list from a user having such a privilege was actually received from that user by sending a confirming email. In other words, no "challenge question" is needed as the confirmation is sent to a known email that is presumed to belong to the actual user, just in case someone else has presented themselves as the user. As such, even were the confirmatory email to be considered a "challenge question" it only serves such a function when it is not sent to the user that submitted the registration request. Accordingly, the rejection of independent Claim 1 and the claims depending therefrom should be also withdrawn for at least these additional reasons.

Independent Claims 13 and 25 contain corresponding recitations. Accordingly, the rejections of independent Claims 13 and 25 and the claims depending therefrom should be withdrawn for at least substantially similar reasons.

The Dependent Claims:

The dependent claims are patentable at least based on the patentability of the independent claims from which they depend. In addition, various of the dependent claims are also separately patentable. For example, newly added Claims 29-31 each recite "wherein the challenge question comprises the user's mother's maiden name, the user's favorite color, the user's favorite brand of cereal and/or at least a portion of the user's telephone number." Such recitations are supported, for example, by the specification at page 1, lines 28-29 and Figure 9B. The confirmatory email of Bansal clearly does not include any of the recited questions. Accordingly, Claims 29-31 are also separately patentable for at least these reasons. Newly added Claims 26-28 recite that the self-service application is for network password management. The Office Action does not even allege such is taught by Bansal. Accordingly, Claims 26-28 are also separately patentable for at least these reasons.

Applicants note the rejections of Claims 9 and 10 further cite to O'Connell, which relates to an automated password reset system using stored questions and answers to control resetting of a user's password. Thus, O'Connell, unlike the confirmatory email of Bansal relied on in rejecting the independent claims, relates to a password management application for a computer user's account, not to management of the use of the benefits (listserv subscriptions of Bansal) of the user's account. As discussed above with respect to the patentability of the independent claims, such are distinct purposes. Therefore, one of skill in the art would not be motivated to incorporate the question and answer procedure of O'Connell into the list registration system of Bansal. Instead of saving questions and associated answers generated by a user, Bansal simply uses a known email for the user, or separate log-in through a website, to confirm registration. In neither case is there any suggestion of issuing challenges to a user, thus making the system of O'Connell an unnecessary addition to the system of Bansal that would merely increase the burden to a user of using the system of

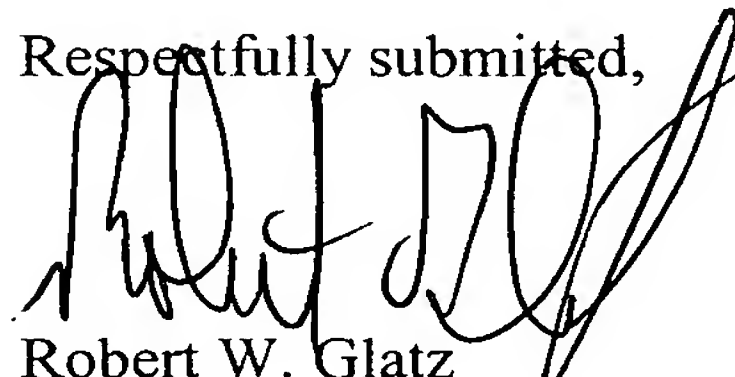
In re: Lineman
Serial No.: 01/696,098
Filed: October 29, 2003
Page 11

Bansal. Thus, Claims 9 and 10 are also separately patentable for substantially the same reasons as Claims 26-28 are separately patentable.

Conclusion

In light of the above remarks, Applicants respectfully submit that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,



Robert W. Glatz
Registration No. 36,811

Customer No. 20792
Myers Bigel Sibley & Sajovec
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401

Certificate of Mailing under 37 CFR § 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on September 13, 2007.



Carey Gregory

DoD 5200.28-STD



Supersedes
CSC-STD-001-83, dtd 15 Aug 83
Library No. S225,711

DEPARTMENT OF DEFENSE STANDARD

DEPARTMENT OF
DEFENSE
TRUSTED COMPUTER
SYSTEM EVALUATION
CRITERIA

DECEMBER 1985

December 26, 1985

FOREWORD

This publication, DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," is issued under the authority of an in accordance with DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," and in furtherance of responsibilities assigned by DoD Directive 5215.1, "Computer Security Evaluation Center." Its purpose is to provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies in support of the overall ADP system security policy, evaluation and approval/accreditation responsibilities promulgated by DoD Directive 5200.28.

The provisions of this document apply to the Office of the Secretary of Defense (ASD), the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, the Defense Agencies and activities administratively supported by OSD (hereafter called "DoD Components").

This publication is effective immediately and is mandatory for use by all DoD Components in carrying out ADP system technical security evaluation activities applicable to the processing and storage of classified and other sensitive DoD information and applications as set forth herein.

Recommendations for revisions to this publication are encouraged and will be reviewed biannually by the National Computer Security Center through a formal review process. Address all proposals for revision through appropriate channels to: National Computer Security Center, Attention: Chief, Computer Security Standards.

DoD Components may obtain copies of this publication through their own publications channels. Other federal agencies and the public may obtain copies from: Office of Standards and Products, National Computer Security Center, Fort Meade, MD 20755-6000, Attention: Chief, Computer Security Standards.

Donald C. Latham
Assistant Secretary of Defense
(Command, Control, Communications, and Intelligence)

Least Privilege - This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

» RESEARCH BRIEFCASE

This Research Briefcase will provide access to all the content you've requested.

 FREE MEMBERSHIP - Create your per

Sep 11, 2007

[Free Newsletters](#)[Most Popular Reports](#)[Top To](#)Search Bitpipe: [Go!](#)[IT Management](#) > [Systems Operations](#) > [Security](#) > [AAA](#) > [Authorization](#) > [Access C](#)

Access Rights

-- [2 Vendor Reports](#) | [1 Product](#)**ALSO CALLED:** Privileges

DEFINITION: In the administration of a multi-user computer system, a privilege is system resource, such as a file folder, the use of certain system commands, or an ar the case of network resources such as access to a particular device, a network admin Definition continues below.

RECENT VENDOR REPORTS ON ACCESS RIGHTS

Least-Privilege: Uses and Consequences

sponsored by BeyondTrust Corporation

WEBCAST: **Posted:** 01 Jun 2007 | **When:** Available On Demand

SUMMARY: The root cause of insecurity is too much access. In this webcast learn how GPOs(Group Policy objects) and other tools to give the right access to the right people
[Briefcase](#)

TOPICS: [Access Control Software](#) | [Access Rights](#) | [Active Directory](#) | [Authentication](#) | [Group P](#)
[Threats](#) | [Windows Security](#) | [Windows Vista](#)

Privileged User Monitoring for SOX Compliance

sponsored by Tizor

WHITE PAPER: **Posted:** 21 Aug 2006 | **Published:** 01 Aug 2006

SUMMARY: This paper outlines a best-practices approach to monitoring and reporting user access activity, failed logins and other access failures, direct Data SQL Access ex changes. [Add to Briefcase](#)

TOPICS: [Access Rights](#) | [Compliance Audits](#) | [Compliance Best Practices](#) | [Compliance Softwa](#)
[Database Administration](#) | [Database Administrators](#) | [Database Security](#) | [IT Auditing](#) | [Sarbanes](#)
[Compliance](#)

ACCESS RIGHTS DEFINITION (continued): ... In the administration of a multi-use particular user has to a particular system resource, such as a file folder, the use of ce Generally, a system administrator or, in the case of network resources such as access privileges to users. System software then automatically enforces these privileges. Access Rights definition sponsored by SearchExchange.com, powered by WhatIs.com

[Home](#) | [About Us](#) | [Contact Us](#) | [Advertise with Us](#) | [Partner with Us](#) | [Site Index](#)

TechTarget provides enterprise IT professionals with the information they need to perform IT purchase decisions and managing their organizations' IT projects - with its network of te



DIGITAL CAMERAS LAPTOPS MP3 PLAYERS CELL PHONES PRINTERS DESKTOPS HDTVS

Sign In | Reg

Collaborate

Train

HOME

REVIEWS

Ask Loyd

Ask Neil

Encyclopedia

SEARCH

PCMAG.COM

EXPERT HELP

SAVE BIG ON PC MAGAZINE!

THE INDEPENDENT GUIDE TO TECHNOLOGY

GET 25 ISSUES FOR ONLY \$19.97!

Name

Address

City

State

Zip

Country

Email

buy now

SEARCH

High-Tech Hollywood

THE BEST FREE SOFTWARE

34 GREAT NEW APPS

etings™

MADE EASY

TRY IT FREE

CLICK HERE

SHOP

DISCUSS

@WORK

Hot Camp

Software

Hardware


PC Magazine:


Current Issue

Previous Issues

Home > Expert Help > Encyclopedia > least privilege

AD





encyclopedia

Over 20,000 IT Terms

Search:

Search Encyclopedia

Browse the index

Definition of: least privilege

A basic principle in information security that holds that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions. For example, the restrictive "need-to-know" approach defines zero access by default and then opens security as required. All data in a corporate network would be off-limits except to specific people or groups (see role-based access control).

In contrast, a less-restrictive strategy opens up all systems and closes access as required; for example, allowing employees access to all systems except human resources and accounting, which would be limited to only employees in those departments.

RELATED TERMS:
role-based access control

Search:

Search Encyclopedia

Browse the index

Microsoft Press

Computer Dictionary

Third Edition

Microsoft Press



PUBLISHED BY

Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 1997 by Microsoft Corporation

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Cataloging-in-Publication Data
Microsoft Press Computer Dictionary. -- 3rd ed.

p. cm.

ISBN 1-57231-446-X

1. Computers--Dictionaries. 2. Microcomputers--Dictionaries.

I. Microsoft Press.

QA76.15.M54 1997

004'.03--dc21

97-15489

CIP

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QMQM 2 1 0 9 8 7

Distributed to the book trade in Canada by Macmillan of Canada, a division of Canada Publishing Corporation.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office. Or contact Microsoft Press International directly at fax (425) 936-7329.

Macintosh, Power Macintosh, QuickTime, and TrueType are registered trademarks of Apple Computer, Inc. Intel is a registered trademark of Intel Corporation. DirectInput, DirectX, Microsoft, Microsoft Press, MS-DOS, Visual Basic, Visual C++, Win32, Win32s, Windows, Windows NT, and XENIX are registered trademarks and ActiveMovie, ActiveX, and Visual J++ are trademarks of Microsoft Corporation. Java is a trademark of Sun Microsystems, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners.

Acquisitions Editor: Kim Fryer

Project Editor: Maureen Williams Zimmerman, Anne Taussig

Technical Editors: Dail Magee Jr., Gary Nelson, Jean Ross, Jim Fuchs, John Conrow, Kurt Meyer, Robert Lyon, Roslyn Lutsch

optimum performance. Peripherals can be connected while the computer is running (*hot plugging*) and are automatically assigned a unique address (auto-addressing). Developed by Digital Equipment Corporation, the ACCESS.bus competes with Intel's USB. *See also* bidirectional, bus, daisy chain, hot plugging, input/output port, peripheral. *Compare* USB.

access code \ak'ses kōd\ *n.* *See* password.

access control \ak'ses kən-trōl\ *n.* The mechanisms for limiting access to certain items of information or to certain controls based on users' identity and their membership in various predefined groups. Access control is typically used by system administrators for controlling user access to network resources, such as servers, directories, and files. *See also* access privileges, system administrator.

access control list \ak'ses kən-trōl list\ *n.* A list associated with a file that contains information about which users or groups have permission to access or modify the file. *Acronym:* ACL (A'C-L').

accessibility \ak-ses'ə-bil'ə-tē\ *n.* The quality of a system incorporating hardware or software that makes it usable by people with one or more physical disabilities, such as restricted mobility, blindness, or deafness.

access mechanism \ak'ses mek'ə-niz-əm\ *n.* 1. The disk drive components that move the read/write head(s) to the proper track of a magnetic disk or optical disc. 2. A circuit that allows one part of a computer system to send signals to another part. *See also* disk controller. 3. In programming, the means by which an application can read from or write to a resource. *Also called* access method.

access method \ak'ses meth'əd\ *n.* *See* access mechanism (definition 3).

access number \ak'ses num'bər\ *n.* The telephone number used by a subscriber to gain access to an online service.

accessory \ak-ses'ər-ē\ *n.* *See* peripheral.

access path \ak'ses path\ *n.* The route followed by an operating system to find the location of a stored file. The access path begins with a drive or volume (disk) designator, continues through a chain of directories and subdirectories, if any, and

ends with the filename. C:\books\diction\start.exe is an example of an access path.

access privileges \ak'ses priv'ə-lə-jəz, priv'lə-jəz\ *n.* The type of operations permitted a given user for a certain system resource on a network or a file server. A variety of operations, such as the ability to access a server, view the contents of a directory, open or transfer files, and create, modify, or delete files or directories, can be allowed or disallowed by the system administrator. Assigning access privileges to users helps the system administrator to maintain security on the system, as well as the privacy of confidential information, and to allocate system resources, such as disk space. *See also* file protection, file server, permission, system administrator, write access.

access provider \ak'ses prə-vī'dər\ *n.* *See* ISP.

access rights \ak'ses rīts\ *n.* The permission to view, enter, or modify a file, folder, or system.

access speed \ak'ses spēd\ *n.* *See* access time.

access time \ak'ses tīm\ *n.* 1. The amount of time it takes for data to be delivered from memory to the processor after the address for the data has been selected. 2. The time needed for a read/write head in a disk drive to locate a track on a disk. Access time is usually measured in milliseconds and is used as a performance measure for hard disks and CD-ROM drives. *See also* read/write head, seek time, settling time, wait state. *Compare* cycle time.

account \ə-kount\ *n.* 1. A record-keeping arrangement used by the vendor of an online service to identify a subscriber and to maintain a record of customer usage for billing purposes. 2. A record kept by local area networks and multi-user operating systems for each authorized user of the system for identification, administration, and security purposes.

accounting file \ə-koun'tēng fīl\ *n.* A file generated by a printer controller that keeps track of the number of pages printed per job as well as the user that requested the print job.

accounting machine \ə-koun'tēng mə-shēn\ *n.* 1. One of the earliest applications of automatic data processing, used in business accounting primarily during the 1940s and 1950s. The first accounting machines were nonelectronic and

Priority Frame

priorities that indicate how soon they must be transmitted. *See also* interrupt.

Priority Frame \prī-ōr'ə-tē frām\ *n.* A telecommunications protocol developed by Infonet and Northern Telecom, Inc., designed to carry data, facsimile, and voice information.

privacy \prī-və-sē\ *n.* The concept that a user's data, such as stored files and e-mail, is not to be examined by anyone else without that user's permission. A right to privacy is not generally recognized on the Internet. Federal law protects only e-mail in transit or in temporary storage, and only against access by Federal agencies. Employers often claim a right to inspect any data on their systems. To obtain privacy, the user must take active measures such as encryption. *See also* encryption, PGP, Privacy Enhanced Mail. *Compare* security.

Privacy Enhanced Mail \prī-və-sē en-hansd' māl\ *n.* An Internet standard for e-mail systems that use encryption techniques to ensure the privacy and security of messages. *Acronym:* PEM (P'E-M'). *See also* encryption, standard. *Compare* PGP.

Private Branch Exchange \prī-vət branch' eks-chānj\ *n.* *See* PBX.

private channel \prī-vət chan'əl\ *n.* In Internet relay chat (IRC), a channel reserved for the use of a certain group of people. Private channel names are hidden from view by the public at large. *Also called* secret channel. *See also* IRC.

Private Communications Technology \prī-vət kə-myōō'nə-kā'shənz tek-nol'ə-jē\ *n.* A specification designed to secure general-purpose business and personal communications on the Internet, and including features such as privacy, authentication, and mutual identification.

private folders \prī-vət fōl'dərz\ *n.* In a shared network environment, those folders on a user's computer that are not currently accessible by other users on the network. *Compare* public folders.

private key \prī-vət kē\ *n.* One of two keys in public key encryption. The user keeps the private key secret and uses it to encrypt digital signatures and to decrypt received messages. *See also* public key encryption. *Compare* public key.

private line \prī-vət līn\ *n.* *See* dedicated line (definition 1).

privatization \prī-və-tə-zā'shən\ *n.* Generally, the process of turning something over from gov-

procedural language

ernment to commercial industry control. In the context of computer science and the Internet, the term refers to the government's turning over of various Internet backbones to private industry. For example, control of NSFnet was passed from the government to private business in 1992.

privileged instruction \priv'ə-ləjd in-struk'shən\ *n.* An instruction (usually a machine instruction) that can be executed only by the operating system. Privileged instructions exist because the operating system needs to perform certain operations that applications should not be allowed to perform; therefore, only the operating-system routines have the necessary privilege to execute these particular instructions.

privileged mode \priv'ə-ləjd mōd\ *n.* A mode of execution, supported by the protected mode of the Intel 80286 and higher microprocessors, in which software can carry out restricted operations that manipulate critical components of the system, such as memory and input/output ports (channels). Application programs cannot be executed in privileged mode; the heart (kernel) of the OS/2 operating system can be, as can the programs (device drivers) that control devices attached to the system.

privileges \priv'ə-lə-jəz, priv'lə-jəz\ *n.* *See* access privileges.

PRN \P'R-N\ *n.* The logical device name for *printer*. A name reserved by the MS-DOS operating system for the standard print device. PRN usually refers to a system's first parallel port, also known as LPT1.

probability \prob'ə-bil'ə-tē\ *n.* The likelihood that an event will happen, which can often be estimated mathematically. In mathematics, statistics and probability theory are related fields. In computing, probability is used to determine the likelihood of failure or error in a system or device.

problem solving \pro'bləm sol'veng\ *n.* 1. The process of devising and implementing a strategy for finding a solution or for transforming a less desirable condition into a more desirable one. 2. An aspect of artificial intelligence wherein the task of problem solving is performed solely by a program. *See also* artificial intelligence.

procedural language \prə-sē'jər-əl lang'wəj\ *n.* A programming language in which the basic pro-

